EXHIBIT H

**IN THE SUPERIOR COURT OF FULTON COUNTY**
**STATE OF GEORGIA**

DONNA CURLING, an individual, et al. )
)
Plaintiffs, )
)
v. ) CIVIL ACTION
) FILE NO.: 2017cv292233
BRIAN P. KEMP, in his individual capacity )
and his official capacity as Secretary of )
State of Georgia and Chair of the )
STATE ELECTION BOARD, et al., )
)
Defendants. )

## DECLARATION OF BARBARA SIMONS

**BARBARA SIMONS** ("Declarant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am computer scientist. I was a Research Staff Member at IBM Research. I subsequently worked as a researcher at IBM's Application Development Technology Institute, followed by time working as a Senior Technical Advisor at IBM Global Services.
2. I am the past Chair and current President of Verified Voting. I am also a former President of the Association for Computing Machinery, the world's largest and oldest educational and scientific computing society.
3. I co-authored *Broken Ballots: Will Your Vote Count?*, a book on voting technology. I wrote the chapter on Diebold that lists the many studies that repeatedly demonstrated the insecurities of Diebold DREs.
4. My curriculum vitae is attached as Exhibit A.

**Opinions of other experts**

5. I have reviewed the affidavit of Edward Felten filed with this court on July 3, 2017 and reviewed the basic structure of Georgia's DRE-based voting system. I concur

with the facts and opinions regarding Georgia's voting DRE voting system as presented in the Felten affidavit.

6. I have reviewed the affidavit of Duncan Buell dated June 29, 2017 and filed with this court on July 3, 2017. I concur with the facts and opinions regarding Georgia's DRE-voting system as presented in the Buell affidavit.

**Background related to Georgia's 6th District Congressional Elections**

7. Upon learning of the March 1, 2017 compromise of the Center for Election Systems servers containing sensitive election files, I helped to organize the March 15, 2017 letter to Secretary of State Kemp from 21 technology experts expressing our serious concerns regarding the safety and accuracy of Georgia's DRE-based voting system. (Exhibit B.)

8. After the April 15, 2017 alleged theft of poll books and the April 18 Fulton County memory card uploading issues, I helped to organize the May 24, 2017 follow up letter from16 technology experts to Secretary Kemp expressing our grave concerns about the escalating risks of Georgia's paperless voting system, and urged the use of paper ballots. (Exhibit C.)

9. The information published in the June 14, 2017 Politico article (http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255) concerning the long-term exposed nature of the CES server and its contents was alarming to me, furthering my grave concerns about Georgia's voting system.

10. I have reviewed Logan Lamb's affidavit concerning his access to the system and filed with this court July 3, 2017.

11. The facts leading up to the 2017 created an undeniable necessity for Georgia's election officials to conduct the April 18 and June 20 special elections presuming that the DRE-based system had been compromised and could not be reasonably relied on for a valid election.

12. I was gravely disappointed that Secretary Kemp and Georgia's 6th Congressional District election officials chose not to conduct verifiable elections with paper ballots after the serious warnings of numerous respected voting system experts.

13. I have researched DRE voting systems since 2003.

14. I have published my research with consistent findings that DRE machines cannot produce a reliable, auditable, re-countable results that provide assurance that voter intent is recorded and tabulated.
15. I concur with the findings of the National Institute of Standards and Technology (NIST) in their January, 2011 report on the work of the Auditability Working Group of the Technical Guidelines Development Committee prepared for the Election Assistance Commission. (https://www.eac.gov/assets/1/28/AuditabilityReport_final_January_2011.pdf)
16. Of particular importance and applicability to Georgia's Special Elections is the NIST Executive Summary statement: "The Auditability Working Group found no alternative that does not have as a likely *consequence* either an effective requirement for paper records or the possibility of undetectable errors in the recording of votes."
17. The "likely consequence" of undetectable errors in Georgia's unverifiable voting results became all the more likely when fundamental security requirements were violated by Georgia officials, causing the results of the recent elections to be unreliable.

**Opinions related to use of DRE's in the 6th Congressional District Special Elections**

18. The possibility and plausibility of undetectable errors has always existed in Georgia's DRE-based system. However, the risk of undetected and undetectable errors has been exponentially increased by the fact that the system has shown to be exposed to cybersecurity threats at an unexpected level.
19. The cybersecurity threats are heightened not only by the extreme risk caused by the inexplicably lax security at CES, but by the routine practices in Georgia of exposing memory cards and GEMS to equipment connected to the internet, and by lax physical security practices in storage of DRE machines when not in use.
20. The multiple security lapses must be presumed to have caused undetectable manipulation of the tabulation results, which cannot be viewed with any reasonable degree of certainty.

21. Georgia's DRE equipment used in the Special Elections could not be reasonably evaluated prior to the Special Elections to determine whether the votes can be read correctly and accurately.

22. County level and precinct level election officials cannot fulfill their duty to determine that the DRE machines have no votes recorded on them before each machine is opened for voting. That is because the voting machines are essentially computers. Computers consist of distinct elements, such as the display (the screen), the memory, and the input mechanism (in this case the touch screen). These elements communicate via communication channels. If a computer's software (firmware) contains software bugs or malicious software, the computer memory could store votes for Candidate A before the election begins, but the software (firmware) could instruct the printer to print wrongly that no votes have been recorded.

23. It is quite unlikely that standard physical security procedures in place in Georgia can prevent the operation of the "counting machinery" when it is stored and not in use. The "counting machinery" is subject to undetectable manipulation through physical or electronic intrusion.

24. County and precinct election officials charged with the duty to determine whether the machines count votes accurately cannot use the pre-election Logic and Accuracy Testing to make this determination because it is possible to detect when Logic and Accuracy testing is occurring and to program the voting machine to behave correctly during the testing, but to cheat during the election. This is how Volkswagen illegally passed emission tests with cars that were significantly polluting: the cars were programmed to limit the amount of harmful emissions (behave correctly) during the testing, but to allow the harmful emissions (cheat during the election) while driving. The same type of approach could be used with voting machines.

25. County and precinct officials cannot meet their duty to "thoroughly test" the machines because malware potentially loaded on the machines would rarely be detectable in standard testing.

26. County and precinct officials cannot reasonably certify that each machine is working properly because standard testing would not permit officials to determine whether each machine is working properly. Sophisticated malware would likely serve to

operate the machine properly when it is being tested, and operate in malicious ways during the election.

27. County and precinct officials cannot fulfill their duty to determine whether votes are already recorded in the machine memory card prior to opening of the polls. "Zero tape" print outs can be programmed to print -0- when the machine contains maliciously implanted votes.

28. If the machines have not been maintained and stored under continuous strict secured physical control prior to and after their use during voting, they are subject to relatively easy entry and manipulation, and must be presumed to be compromised. In such case, local election officials cannot determine whether the machines have been compromised.

29. The GEMS server, (DRE related equipment), is not secure when flash drives (memory cards) are moved between the GEMS server and internet-connected computers, as is the common practice on Election Night.

30. The GEMS servers are not secure when databases and memory cards used on the counties' GEMS servers have been exposed to the Internet as they apparently were through the CES server. Such voting system components must be presumed to have compromised the 2017 Special Elections.

31. Standard testing procedures and routine evaluation of Georgia's voting equipment are inadequate to detect malware in the voting system, or manipulation of results.

32. Because of the foregoing facts, results of Georgia's recent elections using the DRE-based voting system should not be relied on as accurate, and reflecting the intent of the voters.

33. Because Georgia's unverifiable voting system was repeatedly exposed to the Internet and other sources of potential intrusion and manipulation, the equipment should be taken out of service immediately.

Further Declarant sayeth not.

Barbara Simons

# Curriculum Vitae
# Barbara Simons

650.328.8730 voice / 215.243.8002 fax
simons@acm.org

## Education

- Ph.D., Computer Science, the University of California, Berkeley, June 1981 - thesis advisor Richard Karp. My dissertation, *Scheduling with Release Times and Deadlines*, solved a major open problem in scheduling theory by developing the first known algorithm for the problem.

## Employment

- Co-author with Doug Jones, *Broken Ballots: Will Your Vote Count?*, April 15, 2012.
- Consulting Professor, Stanford University, April 2001 – June 2002; taught courses on Internet technology policy; supervised several students in independent study.
- Retired, IBM, 1998.
- Senior Technology Advisor, IBM Global Services, IBM Corp., Nov. 1996 – 1998; worked with researchers and business people to develop and apply research to business problems.
- Researcher, Application Development Technology Institute, IBM Corp., Oct. 1992 – Nov. 1996; did research on compiler optimization and development of a prototype retargeting compiler backend.
- Research Staff Member, Foundations of Computer Science Group, IBM Research, Jan.1980 – Sept. 1992; did research on scheduling theory, compiler optimization, fault tolerant distributed computing, and communicating sequential processes.
- Visiting Professor, U.C. Santa Cruz, Sept. 1984 – Dec. 1984; taught graduate algorithms course.

## Honors

- Walnut Hills High School Hall of Fame Award, Cincinnati, Ohio, April 30, 2011.
- The Making a Difference Award, Special Interest Group on Computers and Society, 2006.
- Distinguished Alumni Award, College of Engineering, U.C. Berkeley, 2005.
- Computing Research Association's Distinguished Service Award, 2004.
- ACM Outstanding Contribution Award, 2002.
- Distinguished Alumnus Award in Computer Sciences and Engineering, U.C. Berkeley, May 21, 2000.
- Selected as one of the top 25 Women on the Web, 2001, by San Francisco Women on the Web.
- Electronic Frontier Foundation (EFF) Pioneer Award 1998.
- Selected as one of 26 Internet "Visionaries" by c|net, Dec. 1995.
- Selected as one of the Top 100 Women in Computing by Open Computing, Dec. 1994.
- Fellow, ACM, elected 1993.
- Fellow, American Association for the Advancement of Science (AAAS), elected 1993.
- Featured in special issue of *Science* on Women in Science, 1992.
- Computer Professionals for Social Responsibility (CPSR) Norbert Wiener Award for Professional and Social Responsibility in Computing, 1992.
- IBM Research Division Award for work on clock synchronization, 1988.

## Policy Interactions with Governmental and Quasi-Governmental Organizations

- Member, Board of Advisors of the federal Election Assistance Commission, appointed by Sen. Harry Reid, August 2008.
- Testified before the Massachusetts legislature in support of voting machine audit legislation, October 22, 2007, Boston, MA.
- Testified before the Committee on House Administration in a hearing on Electronic Voting Machines: Verification, Security, and Paper Trails, September 28, 2006, Washington, DC.
- Member, Security Peer Review Group, a panel of experts who were invited by the U.S. Department of Defense's Federal Voting Assistance Program to evaluate the Secure Electronic Registration and Voting Experiment (SERVE). Co-authored, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", with David Jefferson, Aviel Rubin, and David Wagner, released Jan 21, 2004. On Feb. 5, 2004 the Department of Defense announced the cancellation of SERVE because of security concerns.
- Member, Public Interest Registry's .ORG Advisory Council, starting March 2003 – 2006.
- DARPA Panels
  - Member, Information Science and Technology (ISAT) study group on "Security with Privacy", 2002.
  - Member, IPTO workshop on "eDNA: Identification of Origin", Aug. 5-6, 2002.
- Member, National Workshop on Internet Voting, Oct 11-12, 2000, convened at the request of President Clinton. Co-authored with other attendees "Report of the National Workshop on Internet Voting: Issues and Research Agenda", March 2001.
- Runner-up for the North American seat on the Internet Corporation for Assigned Names and Numbers (ICANN) Board, 2000.
- Expert witness, Universal, et al. v. 2600, et al. (the DVD decryption case), July 8, 2000.
- Invited Participant, the White House Conference on the New Economy, Washington, DC, April 6, 2000.
- Member, President's Export Council Subcommittee on Encryption, 1998-2001.
- Member, Information Technology Working Group of the President's Council on the Year 2000 Conversion, 1998 – 2000.
- Testified before Commerce Committee of the California State Senate on encryption, Aug. 26, 1997.
- Testified at hearings before the National Committee on Vital and Health Statistics on privacy issues in the Kennedy-Kassenbaum Bill, San Francisco, CA, June 4, 1997.
- Testified in Social Security Administration hearing: Privacy and Customer Service in the Electronic Age, San Jose State Univ., May 28, 1997.
- Testified in hearing of the Subcommittee of Science, Technology, and Space of the Senate Committee on Commerce, Science, and Transportation on the "Pro-Code" Bill, S.1726, June 26, 1996.
- Testified on Intellectual Property and the Internet before a panel of the Mega-Project III of the Information Infrastructure Task Force (IITF) Advisory Council and the Security Issues Forum of the IITF, Sunnyvale, CA., Oct. 20, 1994.

## Boards and Related Activities

- Board of Directors, Verified Voting Foundation, 2004 – present. Currently President.
- Advisory Council, Overseas Vote Foundation's End-to-End Verifiable Internet Voting Project, 2013 – 2015.

- Board of Advisors, ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), 2008 – 2012.
- Board of Advisors, Electronic Frontier Foundation, 2008 – present.
- Advisory Board, Oxford Internet Institute, Oxford Univ., 2002 – 2006.
- Member, Public Interest Registry's .ORG Advisory Council, 2003 – 2006.
- Board of Directors, Electronic Privacy Information Center, 1998 – 2006. Board Chair, 2005-2006.
- Berkeley Engineering Fund Board of Directors, U.C. Berkeley College of Engineering, 1998 – 2005.
- Advisory Board, Berkeley Foundation for Opportunities in Information Technology, 1999 – present.
- Advisory Board, Public Knowledge, 2001 – 2005.
- Advisory Board, Zeroknowledge Systems Inc., 2000 – 2004.
- Advisory committee, Excellence and Diversity Student Programs, Department of Electrical Engineering and Computer Science, U.C. Berkeley, 1989 – 2004.
- Board of Directors, Math/Science Network, 2002 – 2004.
- Advisory Board, NSF Logging and Monitoring Project (LAMP), Univ. of Michigan, Ann Arbor, Michigan, 2000 - 2002.
- Board of Directors, Council of Scientific Society Presidents, 1998 – 2000.
- Member, steering committee, 21st Century Project, 1995 – 1998.
- Advisory board, the Genome Radio Project and the Telecommunications Radio Project, the Science and Technology Radio Project, 1994 – 95.
- Corporate Affiliates and Advisory Board, Computer Science Division, U.C. Davis, 1991 – 1994.
- Dartmouth Institute for Advanced Graduate Studies, Dartmouth College, 1991 – 1995.
- Member, advisory group, joint ACLU-CPSR projects on a national ID card and privacy, 1989 – 1991.
- Advisory committee, reentry program in computer science, U.C. Berkeley, 1983 - 1989.
- Member, advisory committee at Mills College for the Interdisciplinary Computer Science Program (Masters degree) for returning adults, 1983 - 1986.

## Patents

- Retargeting Optimized Code by Matching Tree Patterns in Directed Acyclic Graphs, with Vivek Sarkar and Mauricio Serrano, patent pending.
- A Method of, System for, and Computer Program Product for Providing Efficient Utilization of Memory Hierarchy through Code Restructuring (Patent number 6839895), with Dz Ching Ju, K. Muthukumar, and Shankar Ramaswamy.
- A System, Method, and Program Product for Loop Instruction Scheduling for Hardware Lookahead, with Vivek Sarkar, patent pending.
- A System, Method, and Program Product for Instruction Scheduling in the Presence of Hardware Lookahead Accomplished by the Rescheduling of Idle Slots (Patent number 5887174), with Vivek Sarkar.
- Decentralized Synchronization of Clocks (Patent numbers 4584643 and 4531185), with Danny Dolev, Joe Halpern, and Ray Strong.

## Selected Publications

- Voting

  - *Broken Ballots: Will Your Vote Count?,* with Doug Jones, Center for the Study of Language and Information, Stanford, CA., June, 2012.
  - Report on Election Auditing, by the Election Audits Task Force of the League of Women Voters of the United States, January, 2009.
  - Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues, co-chaired with Paula Hawthorn, commissioned by ACM's U.S. Public Policy Committee (USACM), February 2006.
  - Why Johnny Can't Vote, *APS* (the American Physical Society) *News,* March 8, 2005, p. 8.
  - Electronic Voting Systems – the Good, the Bad, and the Stupid, *Queue*, 2, 7, Oct 2004, pp. 20 – 26.
  - A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), with David Jefferson, Aviel Rubin, and David Wagner, released Jan 21, 2004. On Feb. 5, 2004 the Department of Defense announced the cancellation of SERVE because of security concerns.
  - Report of the National Workshop on Internet Voting: Issues and Research Agenda, with other workshop members, March 2001, sponsored by the National Science Foundation and published by the Internet Policy Institute.

- Other Policy issues
  - Shrink-Wrapping our Rights, Inside Risks, *Commun. ACM* 43, 8, August 2000, p. 168.
  - To DVD or not to DVD, *Commun. ACM* 43, 5, May 2000, pp. 31 – 32.
  - Trademarking the Net, *Commun. ACM* 43, 3, March 2000, pp. 27 – 28.
  - Regulating Content on the Internet, a chapter in *Capital for Our Time*, Hoover Institution Press, Stanford, CA, 1999, pp. 156 – 174.
  - Melissa's Message, *Commun. ACM* 42, 6, June 1999, pp. 25 – 26. Also in *iMP*, an on-line journal.
  - Starr Wars, *Commun. ACM*, Jan. 1999, pp. 26 – 27. Also in *iMP*.
  - Outlawing Technology, *Commun. ACM*, Oct. 1998, pp. 17 – 18. Also in *iMP*.
  - On Building a Research Agenda for Computer Science, *Commun. ACM*, 34, No. 10, Oct. 1991, pp. 121 – 125.

- Scheduling Theory
  - A Fast Algorithm for Multiprocessor Scheduling of Unit-Length Jobs, with Manfred Warmuth, *SIAM J. on Comput*., 18, No. 4, 1989, pp. 690 – 710.
  - Multiprocessor Scheduling of Unit-Time Jobs with Arbitrary Release Times and Deadlines, *SIAM J. on Comput*., 12, 1983, pp. 294 – 299.
  - Scheduling Unit-Time Tasks with Arbitrary Release Times and Deadlines, with Michael Garey, David Johnson, and Robert Tarjan*, SIAM J. on Comput*., 10, 1981, pp. 256 – 269.

- Compiler Optimization
  - A Fast Heuristic for Loop Parallelization, with Richard Anderson, a special issue of *Parallel Processing Letters*, 4(3), 1994, pp. 281 – 299.
  - Parallel Program Graphs and their Classification, with Vivek Sarkar, Proceedings of the 6th Annual Languages and Compilers for Parallelism Workshop, Portland, OR, Aug. 12 – 14, 1993. Springer-Verlag *Lecture Notes in Computer Science*, Vol. 768, Jan. 1994, pp. 633 – 655.
  - Instruction Scheduling for Compilers, with Krishna Palem, IBM Research Report 8535, Dec., 1991. Written to appear as a chapter in *Optimization in Compilers*, edited by Fran Allen, Barry Rosen, and Kenny Zadeck.

  - Scheduling Time-Critical Instructions on RISC Machines, with Krishna Palem, *Transactions on Programming Languages* (TOPLAS), 15, No. 4, 1993, pp. 632 – 658.

- Fault Tolerant Distributed Computing
  - Dynamic Fault-Tolerant Clock Synchronization, with Danny Dolev, Joseph Halpern, and Ray Strong, *Journal of the ACM* 42:1, 1995, pp. 143 – 185.
  - *Fault Tolerant Distributed Computing*, coedited with Alfred Spector, Springer-Verlag Lecture Notes in Computer Science, Vol. 448, 1990.
  - A New Look at Fault Tolerant Network Routings, with Danny Dolev, Joseph Halpern, and Ray Strong, *Information and Computation*, 72, 1987, pp. 180 – 196.

- Communicating Sequential Processes
  - Static Analysis of Interprocess Communication, with Peter Ladkin, to appear as a monograph in the Lecture Notes in Computer Science series published by Springer-Verlag.
  - Deadlock Detection for CSP-type Communications, with Peter Ladkin, *Proceedings of the Third International Workshop on Responsive Computer Systems*, Sept. 29 – Oct. 1, 1993, Lincoln, NH, pp. 229 – 239; a chapter in *Responsive Computer Systems: Steps Toward Fault-Tolerant Real-Time Systems*, ed. D. Fussell and M. Malek, Kluwer Academic Pub., 1995.

## Invited Talks

- Invited speaker, Mathematical Sciences Research Insititute, Berkeley, Ca., Sept. 16, 2015.
- Invited speaker, League of Women Voters, Manhattan, Kansas, September 15, 2013.
- Invited speaker, "Garantias electorales para el Fortalecimiento de la Democracia", sponsored by the National Registry and Minister of the Interior, Bogota, Colombia, May 22, 2013.
- Invited speaker, the CRA-W/CDC (Computing Research Assoc. Comm. on the Status of Women / Coalition to Diversify Computing) Distinguished Lecture Series, Orlando, FL, March 26, 2013.
- TED talk, "Why Can't we Vote Online?", New York, NY, November 5, 2012.
- Interviewed on Charlie Rose Show, National Public Television, October 4, 2012.
- Distinguished lecture, IBM Research, San Jose, CA., September 12, 2012.
- Invited speaker, Microsoft Research, Redmond, WA, August 8, 2012.
- Keynote, Women in Science and Engineering workshop, Univ. of CA, Berkeley, CA, June 21, 2012.
- EFF "Geek Reading", San Francisco, CA., May 29, 2012.
- Invited speaker, "The Electoral Code that Colombia Needs", sponsored by the United Nations Development Programme, Bogota Colombia, March 1, 2012.
- Invited by the Mayor of Tallinn, Estonia on a fact finding mission of their Internet voting system, July 18 -19, 2011, Tallinn, Estonia.
- Invited speaker, Workshop on e-voting, European Parliament, March 17, 2011, Brussels.
- Speaker, panel on Internet Voting, Internet, Politics, Policy 2010: An Impact Assessment, Oxford Internet Institute, Oxford, UK.
- Invited by U.S. Department of State's Bureau of Interational Information Program to speak on voting technology to representatives of government of Bahrain, March 24, 2010, Seattle, WA.
- Keynote speaker, annual conference of The Consortium for Computing Sciences in Colleges Northwest Region, Ashland, OR, October 10, 2008.
- Speaker, Distinguished Lecture Series, the University of Oregon, Eugene, OR, March 13, 2008.
- Invited speaker, Google, Mountain View, CA., December 7, 2007.

- Speaker, National Institute on Computing and the Law, sponsored by the American Bar Association, San Francisco, CA, June 25 – 26, 2007.
- Speaker, Distinguished Speaker Series, U.C. Santa Cruz, Santa Cruz, CA, March 14, 2007.
- Blair O. and Teresa A. Rieth Lecturer, DePauw University, Greencastle, Indiana, November 1, 2006.
- Speaker, Symposium on 21st Century Copyright Law in the Digital Domain, University of Michigan, Ann Arbor, MI, March 24, 2006.
- Keynote speaker, 10th European Symposium on Research in Computer Security (ESORICS 2005), Milan, Italy, September 12, 2005.
- Speaker, Distinguished Lecture Series on Computation and Society, Harvard Univ., Dec. 16, 2004.
- Speaker, 2004 Industrial Physics Forum of the American Physical Society, IBM Research, Yorktown, NY, Oct 25, 2004.
- Speaker, Gordon Research Conference on Science & Technology, Big Sky, MT., Aug. 16, 2004.
- Plenary speaker, 25th Anniversary Celebration, Informatics Division, Universitaet Bremen, Bremen, Germany, Oct. 10, 2003.
- Speaker, 2003 Financial Markets Conference – Business Method Patents and Financial Services, sponsored by the Federal Reserve Bank of Atlanta, Sea Island, GA., April 2-5, 2003.
- Speaker, The Public Voice in the Digital Economy Conference, in conjunction with the OECD-APEC Global Forum: Policy Frameworks for the Digital Economy, Honolulu, HI, Jan 14, 2003.
- Plenary speaker, International Symposium on Computer and Information Sciences, Orlando, FL, Oct 28-30, 2002.
- Keynote, IT Career Events for Indiana Women, Oct. 22, 2002.
- Plenary session, *Casting a Wider Net: Integrating research and policy on the social impacts of the Internet*, conference inaugurating the Oxford Internet Institute, Oxford, England, Sept. 27, 2002.
- Plenary speaker, Management of Digital Rights, Germany, Nov. 20 – 21, 2000.
- Speaker, World Knowledge Forum, South Korea, Oct. 18 – 19, 2000.
- Keynote Panelist, Grace Hopper Conf. on the Future of Computing, Sept 16, 2000, Cape Cod, MA.
- Keynote, S. Africa, SAICSIT'99 (The South African Institute for Computer Scientists and Information Technologists), Johannesburg, South Africa, Nov. 17 – 19, 1999.
- Other talks on computerized voting
    - Panelist, Voter Registration Databases, Electronic Verification Network Conference, San Diego, CA, March 6, 2014.
    - League of Women Voters, California Convention, May 18, 2013.
    - Mills College, April 11, 2013.
    - Distinguished lecture: Clemson Univ., Wofford College, Furman College, Winthrop, Univ., (South Carolina), and Univ. of Iowa, Iowa City, Iowa, Feb. 17 – 22, 2013.
    - Panelist, EVT/WOTE conference, Bellvue, WA, August 7, 2012.
    - “Voice of the Voters!”, Philadelphia, PA (and the internet), April 30, 2008.
    - Tufts University, Boston, MA, October 24, 2007.
    - Boston University, Boston, MA, October 23, 2007.
    - *E-voting*, panelist, 1st Annual National Institute on Computing and The Law, sponsored by the American Bar Association, San Francisco, CA, June 25- 26, 2007.

  - Plenary session, *Electronic Voting Integrity*, Computers, Freedom, and Privacy Conference, Montreal, Canada, May 4, 2007.
  - *Are We a Democracy? Vote-Counting in the US*, panelist at AAAS Annual Meeting, San Francisco, CA, February 16, 2007.
  - *Voting Databases*, panelist at Computers, Freedom, and Privacy Conference, Washington, DC, May 4, 2006.
  - University of California at Davis, Davis, CA, March 3, 2005.
  - University of Virginia Law School, Charlottesville, VA, February 6, 2005.
  - University of Michigan, Ann Arbor, MI, Oct. 5, 2004.
  - Center for Discrete Mathematics and Theoretical Computer Science, Rutgers Univ., Piscataway, NJ, May 26-27, 2004.
  - San Francisco School of Law, San Francisco, CA., April 21, 2004.
  - Oxford Internet Institute, Oxford, England, March 19, 2004.
  - Cambridge University, Cambridge, England, March 18, 2004.
  - Speaker, Claim Democracy Conference, Nov. 22-23, 2003, Washington, DC.
  - Stanford Law School, Stanford, CA., Oct. 30, 2003.
  - Panelist, Judge A. Leon Higginbotham Memorial Voting Rights Braintrust panel on voting, sponsored by the Congressional Black Caucus, Washington DC, Sept. 26, 2003.

- Intellectual Property and the Net
  - 21st Century Copyright Law in the Digital Domain, Michigan Telecommunications and Technology Law Review Journal sponsored conference, University of Michigan, Ann Arbor, MI, March 24, 2006.
  - SIGGRAPH 2003. San Diego, July 28, 2003.
  - Harvey Mudd College, Dec. 5, 2002.
  - Distinguished Women Lecture Series, Univ. of Maryland, April 10, 2002.
  - National Institute of Standards and Technology (NIST), Feb. 8, 2002.
  - DIMACS Workshop on Management of Digital Intellectual Prop., Rutgers Univ., April 17 – 18, 2000.
  - ABA National Convention, Aug. 8, 1999.
  - Plenary speaker, ACM Special Interest Group on Computer-Human Interaction, May 19, 1999
  - Distinguished Lecture Series, Brown Univ., Feb. 14, 1999.
  - "Intellectual Capital: Business Strategies, Legal Protections, and Global Competitiveness", Hoover Institution (Stanford), June 19, 1997.
  - Univ. of Maryland Distinguished Lecture Series, May 1, 1996.
  - Invited Conference Chair and speaker, Intellectual Property, Patent and Copyright Protection on the Internet, Atlanta, GA, April 29, 1996.

- Privacy, Surveillance, and the USA/PATRIOT Act
  - Univ. of Maryland, April 10, 2002.
  - EDUCAUSE National Conference, Indianapolis, IN., Oct. 30, 2001.
  - Richard Tapia Celebration of Diversity in Computing, Houston, Texas, Oct. 20, 2001.
  - Policy Briefing: Emerging Cyberspace Issues Internet Jurisdiction and Global Privacy Protection, the National Press Club, Washington, DC, June 4, 2001
  - Policy Briefing: The Internet, Privacy and the Open Source Movement, the National Press Club, Washington, DC, June 5, 2000.

  - "The Future of Public Health: implications for Health Information/Communications Systems," sponsored by the Ca. Dept of Health Services and the Nat. Centers for Disease Control, San Diego, Ca., March 6, 1996.
  - World Affairs Council, San Francisco, CA, April 19, 1994.

- Encryption and Computer Security
  - Plenary session speaker, 9th Annual Conference on Computers, Freedom, and Privacy, Washington, DC, April 1999.
  - "Security and Freedom through Encryption Forum (SAFE)," Stanford Univ., July 1, 1996.
  - Networld/Interop Conference, Sept 13, 1994.
  - KPFA radio, Sept. 6, 1994.
  - KQED radio, May 17, 1994.

- National Information Infrastructure
  - DAGS '95 Conference on Electronic Publishing and the Information Superhighway, Boston, MA, June 1, 1995
  - "Issues in Science and Technology Policy," a Brookings Institute Conference for Corporate and Government Managers, Williamsburg, VA, May 21, 1995.
  - Keynote speaker, Computer Science Conference, Nashville, Tenn., Feb. 28, 1995.
  - National Public Radio's Science Friday, Feb. 17, 1995.
  - IBM Boulder TechExpo series, Feb. 11, 1995.
  - National Public Radio's Science Friday, Dec. 10, 1993.

## Association for Computing Machinery and Other Professional Society Activities

- Co-Chair, ACM panel on Databases of Registered Voters, 2005 – 2006.
- Founder and Chair or Co-Chair, ACM Technology Policy Committee (USACM), 1993 – 2005.
- Member, Committee to Diversify Computing, 2002 – present.
- Chair, ACM Internet Governance Committee (ACM-IGC), 2000 – 2003.
- Member, ACM-W (ACM's Committee on Women), 2000 – present.
- ACM President, 1998 – 2000.
- Secretary, Council of Scientific Society Presidents, 1999 – 2000. (Board member 1998 – 2000).
- Member, Computing Research Association (CRA) committee on Public Policy, 1992 – 1996.
- ACM Secretary, 1990 – 1992.
- Member, ACM Committee on Central and Eastern Europe 1990 – 1996.
- Vice-chair, SIGACT (Special Interest Group on Automata and Computability Theory, ACM) 1983 – 1990.
- Member, ACM Government Information Activities Committee, 1989 – 1990.
- Chair, ACM Committee on Scientific Freedom and Human Rights, June, 1987 – 1990.
- Organizer and Chair, SIGACT Science Policy Committee, Nov. 1986 – 1990.

## Miscellaneous Professional Activities

- Invited panelist, AAAS Workshop on Developing a Research Agenda for Electronic Voting Machines, Washington, DC, Sept 17 – 18, 2004.
- Runner up for the N. American Seat on the ICANN (Internet Corporation for Assigned Names and Numbers) Board, 2000.
- Women in Science

  - Invited participant, National Institutes of Health Summits (Achieving XXcellence '99 and AXXS 2000) on Women in Science, Dec. 9 – 10, 1999 and June 2, 2000.
  - Invited participant, National Academy of Engineering Summit on Women in Engineering, May 17 – 18, 1999 and June 2, 2000.
  - Invited participant, Women in Science Summit, The Women's Leadership Institute at Mills College, Sept. 29 – Oct. 1, 1994.
  - Invited participant, Center for the Advancement of Public Policy multi-media CD-ROM project on Women in the Sciences, March 31, 1994.
  - Invited panelist, Forsythe Panel on Women in Computer Science, Stanford Univ., 1986 and 1989.
  - Invited participant, Conference on Women and Computers, sponsored by MIT, Nov. 1984, and May 1985.
- Associate Editor, ACM Transactions on the Internet Technology (TOIT).
- Associate Editor, Journal of Computing and Information (JCI).
- Member, the National Science Foundation's Collaboratives for Excellence in Teacher Preparation program review panel, Washington, D.C., Sept. 9 – 11, 1992.
- Member, the National Science Foundation's Research Initiation Awards panel, Washington, D.C., 1989.
- Invited participant, workshop on Science, Engineering and Ethics: State-of-the-Art, sponsored by the AAAS, Feb. 15 – 16, 1988, Boston, MA.
- Member of the National Research Council's Graduate Fellowship Evaluation Panel in Computer Science, Washington, D.C., 1985 – 1987.

EXHIBIT I

March 15, 2017

The Honorable Brian Kemp
214 State Capitol
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 3rd it was reported that the Federal Bureau of Investigations is conducting a criminal investigation into an alleged cyber attack of the Kennesaw State University Center for Election Systems. According to the KSU Center for Election Systems' website, "the Secretary of State authorized KSU to create a Center for Election Systems, dedicated to assisting with the deployment of the Direct Record Electronic (DRE) voting technology and providing ongoing support."[1] The Center is responsible for ensuring the integrity of the voting systems and developing and implementing security procedures for the election management software installed in all county election offices and voting systems.

The Center has access to most if not all voting systems and software used in Georgia. It also is responsible for programming these systems and accessing and validating the software on these systems. It is our understanding that the Center also programs and populates with voter records the electronic poll books used in polling places statewide. A security breach at the Center could have dire security consequences for the integrity of the technology and all elections carried out in Georgia.

In order for citizens to have faith and confidence in their elections, transparency is crucial, including about events such as the KSU breach, and its extent and severity. While we understand that this investigation is ongoing and that it will take time for the full picture to emerge, we request that you be as forthcoming and transparent as possible regarding critical information about the breach and the investigation, as such leadership not only will be respected in Georgia but also emulated in other states where such a breach could occur. We expect that you are already pursuing questions such as the following, regarding the breach, and trust that you will make public the results of such inquiry:

1. Can you estimate when the attacker breached KSU's system?
2. How did the attacker breach KSU's system?
3. How was the breach discovered?
4. Which files were accessed?
5. Were any files accessed that related to software or "hashes" for the voting machines?
6. Is there any evidence that files were modified? If so, which files?
7. Had KSU begun ballot builds for the upcoming special election?
8. To whom are these attacks being attributed? Could this be an insider attack? Has the FBI identified any suspects or persons of interest?

[1] http://elections.kennesaw.edu/about/history.php

9. Has the FBI examined removable media for the possibility of implanted malware?
10. Has the FBI examined the hash or verification program for tampering?
11. What mitigations are planned for the near- and long-term?

In any state an attack on a vendor providing software and system support with such far-reaching responsibilities would be devastating. This situation is especially fragile, because of the reliance on DRE voting machines that do not provide an independent paper record of verified voter intent. KSU has instead sought to verify the validity of the software on the voting machines by running a hash program on all machines before and after elections in an effort to confirm that the software has not been altered. However, if KSU's election programming were compromised, it is also possible that the verification program could have been modified to affirm that the software is correct, even if it were not. This is a risk of using software to check the correctness of software.

Of course all Georgia elections are important. This month and next include special elections as well. If these upcoming elections are to be run on DREs and e-pollbooks that are maintained and programmed by KSU while the KSU Center for Election Systems is itself the subject of an ongoing criminal investigation, it can raise deep concerns. And today's cyber risk climate is not likely to improve any time soon.

We urge you to provide Georgia's citizens with information they need to confirm before going to vote that their name will appear correctly on the voter rolls, as well as back-up printed voter lists in case anomalies appear. Most importantly, we urge you to act with all haste to move Georgia to a system of voter-verified paper ballots and to conduct post-election manual audits of election results going forward to provide integrity and transparency to all of Georgia's elections. We would be strongly supportive of such efforts and would be willing to help in any way we can.

Sincerely,

Dr. Richard DeMillo
Charlotte B, and Roger C. Warren Professor of Computing
Georgia Tech

Dr. Andrew W. Appel
Eugene Higgins Professor of Computer Science,
Princeton University

Dr. Duncan Buell
Professor, Department of Computer Science & Engineering, NCR Chair of Computer Science & Engineering,
University of South Carolina

Dr. Larry Diamond
Senior Fellow, Hoover Institute and
Freeman Spogli Institute, Stanford University

Dr. David L. Dill
Professor of Computer Science,
Stanford University

Dr. Michael Fischer

Dr. J. Alex Halderman

Professor of Computer Science,
Yale University

Professor, Computer Science and Engineering
Director, Center for Computer Security and Society
University of Michigan

Dr. Joseph Lorenzo Hall
Chief Technologist,
Center for Democracy & Technology

Candice Hoke
Co-Director, Center for Cybersecurity & Privacy Protection and Professor of Law,
Cleveland State University

Harri Hursti
Chief Technology Officer and co-founder, Zyptonite, and founding partner, Nordic Innovation Labs.

Dr. David Jefferson
Lawrence Livermore National Laboratory

Dr. Douglas W. Jones
Department of Computer Science
University of Iowa

Dr. Joseph Kiniry
Principal Investigator, Galois
Principled CEO and Chief Scientist,
Free & Fair

Dr. Justin Moore
Software Engineer, Google

Dr. Peter G. Neumann
Senior Principal Scientist, SRI International Computer Science Lab, and moderator of the ACM Risks Forum

Dr. Ronald L. Rivest
MIT Institute Professor

Dr. John E. Savage
An Wang Professor of Computer Science,
Brown University

Bruce Schneier
Fellow and lecturer
Harvard Kennedy School of Government

Dr. Barbara Simons
IBM Research (retired),
former President Association for Computing Machinery (ACM)

Dr. Philip Stark
Associate Dean, Division of Mathematics and Physical Sciences,
University of California, Berkeley

Dr. Vanessa Teague
Department of Computing & Information systems, University of Melbourne

Affiliations are for identification purposes only, they do not imply institutional endorsements.

EXHIBIT J

May 24, 2017

The Honorable Brian Kemp
214 State Capitol
Atlanta, Georgia 30334

Dear Secretary Kemp,

On March 14th we sent a letter to you expressing grave concerns regarding the security of Georgia's voting systems and requesting transparency from your office concerning key questions about the reported breach at Kennesaw State University Center for Election Systems (KSU).

The FBI has reportedly closed its investigation into the breach at KSU and will not be pressing federal charges[1] but regrettably little more is known. We remain profoundly concerned about the security of Georgia's votes and the continued reliance on Diebold paperless touchscreen voting machines for upcoming elections.[2]

The FBI's decision not to press charges should not be mistaken for a confirmation that the voting systems are secure. The FBI's responsibility is to investigate and determine if evidence exists indicating that federal laws were broken. Just because the FBI concluded this hacker did not cross that line does not mean that any number of other, more sophisticated attackers could not or did not exploit the same vulnerability to plant malicious software that could be activated on command. Moreover, the FBI's statement should not be misinterpreted to conclude that KSU or the Georgia voting system do not have other security vulnerabilities that could be exploited by malicious actors to manipulate votes.

Any breach at KSU's Election Center must be treated as a national security issue with all seriousness and intensity. We urge you to engage the Department of Homeland Security and the US Computer Emergency Readiness Team (CERT) to conduct a full forensic investigation. We cannot ignore the very real possibility that foreign actors may be targeting our election infrastructure.

The FBI investigation lasted a mere few weeks. It's our understanding that this investigation was designed to determine whether criminal charges should be brought. However, a truly comprehensive, thorough and meaningful forensic computer security investigation likely would not be completed in just a few weeks, and it could take many months to know the extent of all vulnerabilities at KSU, if any have been exploited and if those exploits extended to the voting systems. Time and again cyber breaches are found to have been far more extensive than initially reported. When the breach at the Office of Personnel and Management was discovered in March of 2014 it was not disclosed to the public because officials concluded (incorrectly) that there was no loss of personal identifying information. The system was then reviewed by a private security

[1] Torres, Kristina, "Feds: "Security Researcher" behind KSU data breach broke no federal law," *Atlanta Journal Constitution,* March 31, 2017

[2] Diamont, Aaron, "KSU takes back seat in Georgia elections after server hack," *WSB-TV2 Atlanta News,* March 17, 2017

firm which determined in May (again incorrectly) that the system's security was sound.[3] One month later news reports surface warning that 25,000 individuals' personnel records have been compromised. A year later, that number had grown to over 21 million plus the fingerprints of 5.6 million employees.[4]

Problems reported during the April 18th special election have only escalated our concerns. According to news reports, an error occurred during the uploading of votes in Fulton County on election night.[5] Fulton's director of registration and elections, claimed that when a memory card was uploaded to transfer vote totals the operation failed and the system generated an error message that was "gobbledygook, just junk, just letters."[6] This sort of error message could be the result of a corrupted database and more investigation is needed.

While one cause of database corruption could be cyber intrusion which should not be ruled out, it is important to note that it was documented over ten years ago that the Diebold GEMS database used in Georgia is vulnerable to database corruption, especially if databases are run concurrently[7] as reportedly occurred in the recent special election.[8] This is because GEMS was built on Microsoft JETS database software, an outdated database which cannot be relied upon to provide accurate data.

According to Microsoft:

> "*When Microsoft JETS is used in a multi-user environment, multiple client processes are using file read, write, and locking operations on a shared database. Because multiple client processes are reading and writing to the same database and because JETS does not use a transaction log (as do the more advanced database systems, such as SQL Server),* ***it is not possible to reliably prevent any and all database corruption."***[9][Emphasis added.]

The voting system database stores the vote data. Corruption of the database could mean vote data, or vote counts, are lost. Because Georgia still relies on touchscreen voting machines that do not provide a paper ballot, if votes data is corrupted, it is possible that vote totals could be lost and without a physical paper ballot, there is no way to restore and correct the vote count.

This would be an excellent time to move with all expediency to replace Georgia's outdated voting system, to adopt paper ballot voting and implement robust manual post-election audits. The threat that foreign hackers might target the Dutch national elections caused the Netherlands

[3] "Timeline: What We Know about the OPM Breach," *NextGov.com, http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/*

[4] Rosenfeld, Everett, "Office of Personnel and Management: 5.6 million estimated to have fingerprints stolen in breach," *CNBC,* September 23, 2015

[5] Kass, Arielle, "'Rare error' delays Fulton County vote count in 6th district race," *Atlanta Journal Constitution,* April 19, 2017

[6] *Ibid*.

[7] Hoke, Candice, Ryan, Thomas, "GEMS Tabulation Database Design Issues in Relation to Voting System Certification Standards," https://www.usenix.org/legacy/event/evt07/tech/full_papers/ryan/ryan.pdf

[8] Kass, Arielle, "'Rare error' delays Fulton County vote count in 6th district race," *Atlanta Journal Constitution,* April 19, 2017

[9] How to Troubleshoot and to Repair a Damaged Access 2002 or Later Database, (Rev. 6.1 2006) at http://support.microsoft.com/default.aspx?scid=kb;en-us;283849

to cancel all electronic voting and hold its March elections on paper ballots. The U.S. has not responded to the threat of foreign hacking with the same accountability and speed. The former director of U.S, national intelligence James Clapper recently told Congress that foreign hackers will continue to attack and we should expect them in the 2018 and 2020 elections.[10]

We believe this is a profoundly serious national security issue. We stand ready to help you any way we can to help protect our democratic process and regain the confidence of voters.

Sincerely,

Dr. Richard DeMillo
Charlotte B, and Roger C. Warren Professor of Computing
Georgia Tech

Dr. Andrew W. Appel
Eugene Higgins Professor of Computer Science,
Princeton University

Dr. Duncan Buell
Professor, Department of Computer Science & Engineering, NCR Chair of Computer Science & Engineering,
University of South Carolina

Dr. David L. Dill
Professor of Computer Science,
Stanford University

Dr. Michael Fischer
Professor of Computer Science,
Yale University

Dr. J. Alex Halderman
Professor, Computer Science and Engineering
Director, Center for Computer Security and Society
University of Michigan

Candice Hoke
Co-Director, Center for Cybersecurity & Privacy Protection and Professor of Law,
Cleveland State University

Harri Hursti
Chief Technology Officer and co-founder, Zyptonite, and founding partner, Nordic Innovation Labs.

Dr. David Jefferson
Lawrence Livermore National Laboratory

Dr. Douglas W. Jones
Department of Computer Science
University of Iowa

Dr. Joseph Kiniry
Principal Investigator, Galois
Principled CEO and Chief Scientist,
Free & Fair

[10] Ng, Alfred, "Ex-intel chief James Clapper warns of more Russian hacks," *CNET,* May 8, 2017

Dr. Ronald L. Rivest
MIT Institute Professor

Dr. John E. Savage
An Wang Professor of Computer Science,
Brown University

Dr. Barbara Simons
IBM Research (retired),
former President Association for Computing
Machinery (ACM)

Dr. Philip Stark
Associate Dean, Division of Mathematics and
Physical Sciences,
University of California, Berkeley

Dr. Vanessa Teague
Department of Computing & Information systems,
University of Melbourne

Affiliations are for identification purposes only, they do not imply institutional endorsements.

EXHIBIT K

# THE STATE OF GEORGIA

## OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do hereby certify that*

The AccuVote TS R6 and the AccuVote TSX Voting System, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS firmware version 1.94w, Encoder software version 1.32, Key Card Tool 1.01, ExpressPoll 4000 and ExpressPoll 5000 firmware version 2.1.2 with card writer 1.1.4.0, manufactured by Premier Election Solutions, Inc. formerly known as Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Chapter 2 of Title 21 of the Official Code of Georgia; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to ensure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 8th day of May, in the year of our Lord Two Thousand and Eight and of the Independence of the United States of America the Two Hundred and Thirty-Second.

STATE OF GEORGIA
CONSTITUTION
WISDOM JUSTICE MODERATION
1776

Karen C Handel

Karen C. Handel, Secretary of State

THE STATE OF GEORGIA

# OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do hereby certify that*

the attached nine pages, labeled A through I, are true and correct copies of voting equipment certifications; all as same appear on file in this office.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 18th day of April, in the year of our Lord Two Thousand and Eight and of the Independence of the United States of America the Two Hundred and Thirty-Second.

STATE OF GEORGIA 1776

Karen C Handel

Karen C. Handel, Secretary of State

THE STATE OF GEORGIA

# OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do hereby certify that*

the attached one (1) page constitutes a true and correct copy of the certification of the AccuVote TS R6 Voting System, consisting of GEMS Version 1.1822G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, for use by the electors of the State of Georgia in all primaries and elections as provided in Georgia Election Code 21-2; all as same appear on file in this office.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 27th day of November, in the year of our Lord Two Thousand and Seven and of the Independence of the United States of America the Two Hundred and Thirty-Second.

STATE OF GEORGIA
1776

Karen C Handel

**Karen C. Handel, Secretary of State**

B

# THE STATE OF GEORGIA

## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 10th day of July, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.

Cathy Cox

Cathy Cox, Secretary of State

C

# THE STATE OF GEORGIA

## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

For the purposes of a Conditional Interim Certification the AccuVote TS R6 and the AccuVote TSX Voting System, consisting of GEMS version 1.18.24, AVTS firmware version 4.6.4, and AVTS voting stations with the attached AccuView Printer Module (The following components of the Georgia voting system were included in the test to verify compatibility: GEMS 1.18.22G, AccuVote TS R6 voting stations with firmware AVTS 4.5.2, AccuVote TSX voting stations with AccuVote firmware AVTS 4.5.2, and ExpressPoll 4000 1.2.0.), manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; the Conditional Interim Certification shall expire on December 31, 2006.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 9th day of August, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.

Cathy Cox

Cathy Cox, Secretary of State

D

# THE STATE OF GEORGIA

## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 14th day of April, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirtieth.

STATE OF GEORGIA CONSTITUTION

Cathy Cox

Cathy Cox, Secretary of State

E

THE STATE OF GEORGIA

## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.

Cathy Cox

Cathy Cox, Secretary of State

F

THE STATE OF GEORGIA

# OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.

Cathy Cox

Cathy Cox, Secretary of State

G

# THE STATE OF GEORGIA

## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

the AccuVote TS R6 Voting System, consisting of GEMS Version 1.18.22G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software 1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 31st day of December, in the year of our Lord Two Thousand and Four and of the Independence of the United States of America the Two Hundred and Twenty-Ninth.

STATE OF GEORGIA 1776

Cathy Cox

Cathy Cox, Secretary of State

# State of Georgia

STATE OF GEORGIA 1776

## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that* the AccuVote TS R6 Voting System, consisting of GEMS Version 1.18.15, and the AVTS firmware, Version 4.3.14, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

STATE OF GEORGIA 1776

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 10th day of February, in the year of our Lord Two Thousand and Three and of the Independence of the United States of America the Two Hundred and Twenty-ninth

Cathy Cox

SECRETARY OF STATE

I

# State of Georgia

STATE OF GEORGIA 1776

OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that* the AccuVote TS R6 Voting System, consisting of the AVTS firmware, Version 4.1.11, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 23th day of May, in the year of our Lord Two Thousand and Two and of the Independence of the United States of America the Two Hundred and Twenty-sixth

STATE OF GEORGIA 1776

Cathy Cox

SECRETARY OF STATE

EXHIBIT L

The Office of Secretary of State

*Brian P. Kemp*
SECRETARY OF STATE

*C. Ryan Germany*
GENERAL COUNSEL

June 5, 2017

VIA U.S. MAIL

Mustaque Ahamad
898 Kings Ct NE
Atlanta, GA 30306

David Bader
1824 Charline Ave NE
Atlanta, GA 30306

Ricardo Davis
206 Hunters Mill Lane
Woodstock, GA 30188

Richard DeMillo
2500 Peachtree Rd NW
Unit 606
Atlanta, GA 30305

Virginia Forney
59 Park Lane NE
Atlanta, GA 30309

Merrick Furst
1707 Wildwood Rd NE
Atlanta, GA 30306

Adam Ghetti
606 E. Morningside Drive
Atlanta, GA 30324

Jeff Levy
916 Kings Ct., Unit 1201
Atlanta, GA 30306

Rhonda J. Martin
2500 Peachtree Rd NW
Suite 606
Atlanta, GA 30305

Paul Nally
3667 Hwy 140
Rydal, GA 30171

Michael Opitz
1802 Wynfair Ct.
Marietta, GA 30062

Re: Request for Reexamination of Voting System

Dear Electors,

As the electors who requested a reexamination of the direct recording electronic voting system used throughout Georgia, I wanted to update you on how the Secretary of State's office intends to comply with that request in accordance with O.C.G.A. § 21-2-379.2. Such a request has never been made until now, so I appreciate you bearing with us as we determine the best way to undertake a robust and cost-effective reexamination of the system that includes 27,000 voting machines across the state of Georgia.

Your request differs from requests to review direct recording electronic voting systems prior to being used in Georgia, as the system that you seek to have reexamined has already been deployed statewide. Therefore, a reexamination of that system should be broad enough so that a significant confidence level may be had in the final report. We estimate that such a review will cost $10,000 and will take six months to complete. This estimate is subject to revision as we conduct the reexamination.

You also requested a copy of the most recent certification documentation for the current voting system. Copies of those documents are available for you to review at your convenience at the Office of the Secretary of State, Elections Division, 2 MLK Jr. Dr., Suite 802, West Tower, Atlanta, Georgia, 30334.

Thank you for your interest in Georgia's elections.

Sincerely,

C. Ryan Germany

Cc: Marilyn Marks (*marilyn@aspenoffice.com*) via email
Dr. Duncan Buell (*buell@acm.org*) via email

EXHIBIT M

**George Balbona**
180 Mathews Circle, Marietta, Georgia 30067
**Telephone:** (404) 641-9632 **Email:** balbonag@mac.com

June 26, 2017

## PETITION FOR RECANVASS BY ELECTORS IN THE 6th DISTRICT OF GEORGIA

We, citizens of the 6th District of DeKalb County, Georgia, hereby petition a recanvass of all the memory cards (PCMCIA cards) for the following precincts in DeKalb County:

Briarwood
Ashford Park Elem
Kittredge Elem
Cross Keys High
Mt Vernon West

Recounts and Recanvasses are governed by the Rules of the State Election Board of Georgia, Ga Comp. R. & Regs. 183-1-12-.01:

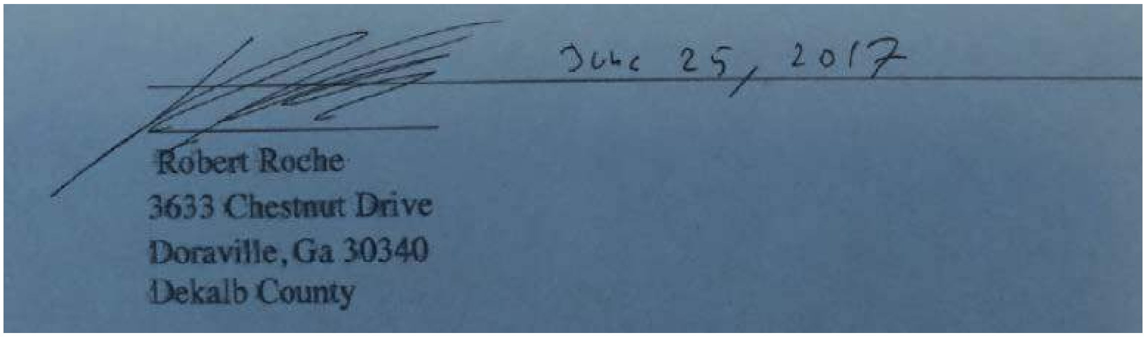
> (7) Recounts and Recanvass.
>
> (a) The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made. Such recanvass may be held at any time prior to the certification of the consolidated returns by the election superintendent and shall be conducted under the direction of the election superintendent. Before making such recanvass, the election superintendent shall give notice in writing to each

> candidate and to the county chairperson of each party or body affected by the recanvass. Each such candidate may be present in person or by representative and each such political party or body may send two representatives to be present at such recanvass. If upon such recanvass, it shall appear that the original vote count was incorrect, such returns and all papers being prepared by the election superintendent shall be corrected accordingly.
>
> (b) The election superintendent shall conduct the recanvass by breaking the seal, if the ballots cards have been sealed, on the container containing the memory cards (PCMCIA cards) and removing those memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted. The election superintendent shall then cause the vote totals on each of the memory cards (PCMCIA cards) to be transferred to either an accumulator DRE unit or to the election management system computer. After all of the vote totals from the memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted have been entered, the election superintendent shall cause a printout to be made of the results and shall compare the results to the results previously obtained. If an error is found, the election superintendent shall correct the error in the returns accordingly.

We, three electors of the 6th District in DeKalb County, Georgia, hereby petition for a recanvass of all of the memory cards for the aforementioned precincts because they may contain errors and discrepancies, which must be examined and corrected.

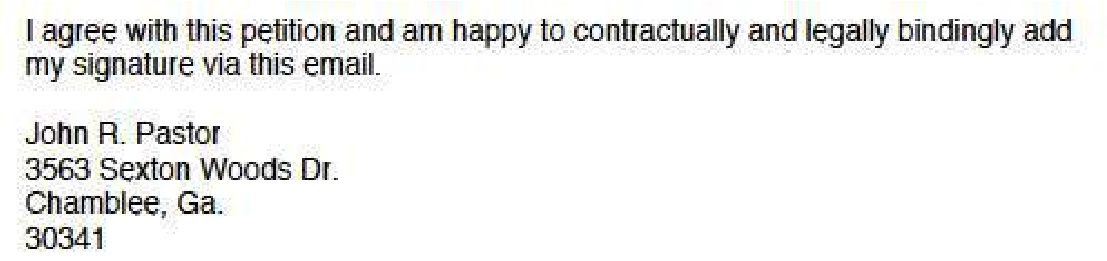
Respectfully submitted,

George Balbona



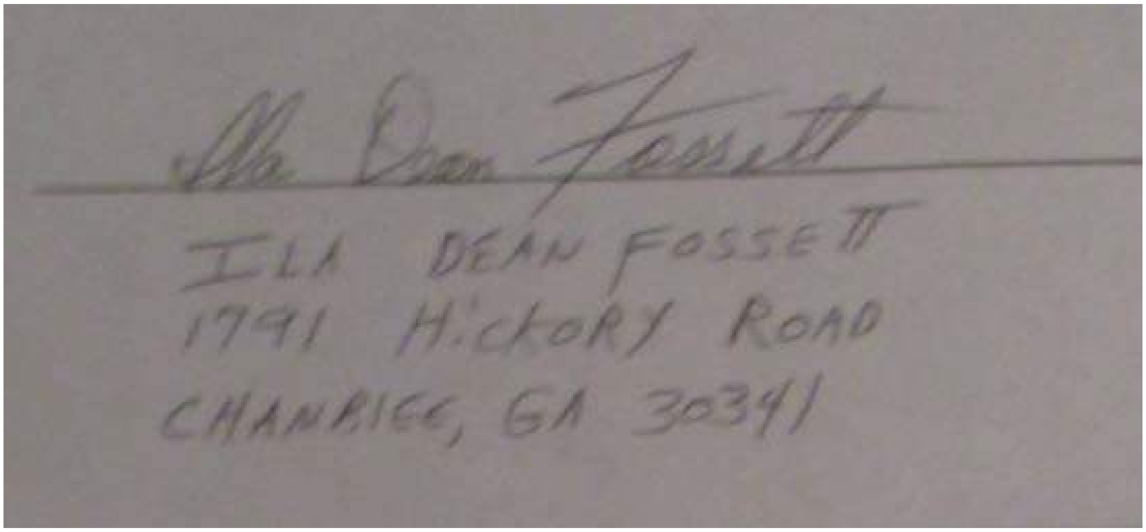
June 25, 2017

Robert Roche
3633 Chestnut Drive
Doraville, Ga 30340
Dekalb County



I agree with this petition and am happy to contractually and legally bindingly add my signature via this email.

John R. Pastor
3563 Sexton Woods Dr.
Chamblee, Ga.
30341



Ila Dean Fossett

ILA DEAN FOSSETT
1791 Hickory ROAD
CHAMBLEE, GA 30341

**George Balbona**
180 Mathews Circle, Marietta, Georgia 30067
**Telephone:** (404) 641-9632 **Email:** balbonag@mac.com

June 26, 2017

## PETITION FOR RECANVASS BY ELECTORS IN THE 6th DISTRICT OF GEORGIA

We, citizens of the 6th District of Cob County, Georgia, hereby petition a recanvass of all the memory cards (PCMCIA cards) for the following precincts in Cobb County:

Chattahoochee 01
Marietta 5A
Marietta 6A
Marietta 6B
Marietta 7A
Powers Ferry 01
Bells Ferry 03
Roswell 01
Mount Bethel 01
Hightower 01
Eastside 02
Murdock 01
Eastside 01
Fullers Park 01

Recounts and Recanvasses are governed by the Rules of the State Election Board of Georgia, Ga Comp. R. & Regs. 183-1-12-.01:

> (7) Recounts and Recanvass.
>
> (a) The election superintendent shall, either of his or her own motion, or upon petition of any candidate or political party or three electors of the county or municipality, as may be the case, order a recanvass of all the memory cards (PCMCIA cards) for a particular precinct or precincts for one or more offices in which it shall appear that a discrepancy or error, although not apparent on the face of the returns, has been made. Such recanvass may be held at any time prior to the certification of the consolidated returns by the election superintendent and shall be conducted under the direction of the election superintendent. Before making such recanvass, the

election superintendent shall give notice in writing to each candidate and to the county chairperson of each party or body affected by the recanvass. Each such candidate may be present in person or by representative and each such political party or body may send two representatives to be present at such recanvass. If upon such recanvass, it shall appear that the original vote count was incorrect, such returns and all papers being prepared by the election superintendent shall be corrected accordingly.

(b) The election superintendent shall conduct the recanvass by breaking the seal, if the ballots cards have been sealed, on the container containing the memory cards (PCMCIA cards) and removing those memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted. The election superintendent shall then cause the vote totals on each of the memory cards (PCMCIA cards) to be transferred to either an accumulator DRE unit or to the election management system computer. After all of the vote totals from the memory cards (PCMCIA cards) for the precinct or precincts for which the recanvass is being conducted have been entered, the election superintendent shall cause a printout to be made of the results and shall compare the results to the results previously obtained. If an error is found, the election superintendent shall correct the error in the returns accordingly.

We, three electors of the 6th District in Cobb County, Georgia, hereby petition for a recanvass of all of the memory cards for the aforementioned precincts because they may contain errors and discrepancies, which must be examined and corrected.

Respectfully submitted,

George Balbona

George Balbona

George Balbona

George Balbona

ALLISON KNOCH
NOTARY PUBLIC
GWINNETT COUNTY, GEORGIA
MY COMMISSION EXPIRES
DECEMBER 21, 2017

Sworn to and submitted before me this 25th day of June, 2017.

Cathy Balbon

Cathy Balbona

ALLISON KNOCH
NOTARY PUBLIC
GWINNETT COUNTY, GEORGIA
MY COMMISSION EXPIRES
DECEMBER 21, 2017

Sworn to and submitted before me this 25th day of June, 2017.

Brian Peters

ALLISON KNOCH
NOTARY PUBLIC
GWINNETT COUNTY, GEORGIA
MY COMMISSION EXPIRES
DECEMBER 21, 2017

Sworn to and submitted before me this 25th day of June, 2017.

EXHIBIT N

**Rocky Mountain Foundation**
7035 Marching Duck Drive E504
Charlotte, NC 28210
704 552 1518
Marilyn@RockyMountainFoundation.org

June 24, 2017

Fulton County Board of Elections
Hand delivered
(Also via email felisa.cordy@fultoncountyga.gov
richard.barron@fultoncountyga.gov
Dwight.Brower@fultoncountyga.gov )

Dear Fulton County Board of Elections:

As you consider the certification of the 6th Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. Fulton County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct of the Superintendent and staff by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, Fulton County officials have been aware of gravely concerning security failures and intrusions, and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in

the June 7 Curling v. Kemp et al. hearing that the security lapses render the system insecure and unfit for the conduct of the election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server. (http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255 ) Fulton officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. On April 18, Fulton County officials exposed the GEMS server and all memory cards to cyber security attack from the Internet by using a common, shared flash drive to upload from the GEMS server to the on-line Clarity ENR system, and then reusing that flash drive in the GEMS server. Such serious lapses in security hygiene must be presumed to have compromised the system, and constitute misconduct on the part of the officials. It cannot be reasonably assumed that the system was safe for vote recording and tabulation, even if this practice had been discontinued on June 20. Exposure to the Internet via shared flash drives undermined the security of the entire election.

   Although regulations require direct upload of memory cards to the GEMS server for official results with the stated intent of avoiding cyber-attacks in election night electronic transmission, the poor security hygiene practices in Fulton County only escalate the risk of cyber-attack. The memory cards and the GEMS server were exposed and made vulnerable during the election night electronic transmission and during the physical upload to the GEMS server after the GEMS server was exposed to the Internet through the irresponsible use of shared flash-drives. Such misconduct cannot be ignored by this board.

3. The Fulton County collection centers' use of TSx machines to transmit votes from TS machines over modem is not a federally approved standard use of the TSx machine, and not certified to be configured, connected and used in this manner, which exposes the memory cards and GEMS server to cyber-attacks during electronic transmission.

4. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. Fulton County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.

5. Physical security of the machines was inadequate prior to the election and during early voting. Given the known exposure of Georgia's system to cyber-attacks and the risk of undetected hacking, it was irresponsible of Fulton County Board and Superintendent to leave machines exposed to easy access by malicious intruders cutting cables and using and replacing tamper-evident seals with identical seals. Although current regulations may permit such risky machine storage in unsecured areas, the board must not irresponsibly rely on permissive and outdated regulations when grave security risks are known to exist. Responsible decisions must be made in light of existing circumstances. If a hallway were flooded with water, machines would not be placed in the water just because the regulations don't prohibit putting machines in flooded areas. Officials have a duty to protect the voting system, and have failed in that duty, in a negligent abuse of discretion.

6. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."

7. On April 18, Fulton County experienced memory card uploading problems to the GEMS server. Officials stated that the GEMS server displayed a message that the upload was successful, with no error messages received until the export of the data from GEMS to the Clarity system. The Superintendent and Board are aware that a functioning, certified GEMS server produces error messages. and does not permit the upload of improper memory cards. This serious problem of no error message signals that the GEMS server is not in safe and proper operational condition, and cannot be relied on to generate accurate election results.

8. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Superintendent must fulfil their legal duty to conduct a secure election free from the threats of a compromised system.

9. Despite the Superintendent's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Superintendent abused his discretion by ignoring multiple expert warnings and conducting the election on a system he knew to be insecure and in violation of laws and regulations. Mr. Barron was present for testimony in the June 7 Curling v. Kemp hearing, and received the pleading including experts' affidavits in that case, and therefore had more than adequate knowledge of the dangers of the uncertified system to require that he employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified. It supplements the petition for paper ballots delivered to this board on May 11. (attached.)

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,

Marilyn Marks
Executive Director
Rocky Mountain Foundation

**Rocky Mountain Foundation**
7035 Marching Duck Drive E504
Charlotte, NC 28210
704 552 1518
Marilyn@RockyMountainFoundation.org

June 26, 2017

Director Daniels and DeKalb County Board of Elections
Hand delivered
(Also via email voterreg@dekalbcountyga.gov )

Dear Director Daniels and DeKalb County Board of Elections:

As you consider the certification of the 6th Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were eligible voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. DeKalb County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election, or the results you plan to certify today.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, DeKalb County officials have been aware of gravely concerning security failures and intrusions, (particularly those at KSU), and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in the June 7 Curling v. Kemp et al. hearing that the security lapses render the system insecure and unfit for the conduct of the

election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server. (http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255 ) DeKalb officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. DeKalb County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.

3. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system.  As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."

4. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Elections Director must fulfil their duty to conduct a secure election free from the threats of a compromised system.

5. Despite the Board's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Director and Board abused their discretion by ignoring multiple expert warnings and conducting the election on a system she knew to be insecure and in violation of laws and regulations. The board was represented by attorneys for testimony in the June 7 Curling v. Kemp hearing, and received the pleadings in that case, and therefore had more than adequate knowledge of the dangers of the uncertified and compromised system to require that Ms.Daniels and the board employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified.

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,

Marilyn Marks
Executive Director
Rocky Mountain Foundation

cc: Bennett Bryan (bdbryan@dekalbcountyga.gov )

**Rocky Mountain Foundation**
7035 Marching Duck Drive E504
Charlotte, NC 28210
704 552 1518
Marilyn@RockyMountainFoundation.org

June 26, 2017

Director Eveler and Cobb County Board of Elections
Hand delivered
(Also via email dwhite@hlclaw.com)

Dear Director Eveler and Cobb County Board of Elections:

As you consider the certification of the 6th Congressional District special election, we respectfully request that you decline to certify the June 20 election results. Rocky Mountain Foundation is a non-profit, non-partisan organization focused on election integrity, and makes this request on behalf of our members who were eligible voters in the June 20 election.

Significant security lapses and system intrusions are known to have plagued the voting system in the months leading up the election. Cobb County election officials have not taken responsible forensic measures to analyze whether the system was safe for use, and in fact, has irresponsibly and repeatedly ignored experts' warnings that the system cannot be considered secure or accurate for the conduct of the June 20 election, or the results you plan to certify today.

The current situation is analogous to a paper ballot election conducted using an unsecured ballot box left open for the entire election with only sporadic oversight. This board would be unable to certify the results of such a paper ballot election because of the security failure of chain of custody of the ballots. The situation today with voters' electronic ballots is no different. The ongoing significant security failures cannot be overcome to permit a certification of the election.

We urge you not to ratify the improper conduct of the Superintendent and staff by certifying the election where legally required controls were absent, security protections failed, and irregularities in the required protocols exist in numerous areas.

The election results should not be certified for several reasons:

1. For several months, Cobb County officials have been aware of gravely concerning security failures and intrusions, and the lack of even a minimally secured voting system. Officials are and have been aware of expert testimony in the June 7 Curling v. Kemp et al. hearing that the security lapses render the

system insecure and unfit for the conduct of the election. It goes without saying that the security failures have placed the results in considerable doubt, and results should not be certified. The extensive level of the security failures was further exposed in press reports before Election Day of the multiple intrusions into the wide-open CES server. (http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255 ) Cobb officials ignored the dire warning the reports provided. Such misconduct on the part of officials must not be exacerbated by certifying the returns.

2. The election has been conducted on an illegal voting system that fails to comply with Georgia's election code and related rules. The Secretary of State has not certified the system currently in use as a voting system that can be used "safely and accurately" as required by §21-2-379.2(a). The most recent system certifications by the Secretary of State office have not addressed the safety and accuracy of the systems as require by statute, nor have such certifications covered the current system configuration. Cobb County has chosen to deploy a collection of components that do not meet either the state statutes for an approved voting system or the Secretary of State's regulations for certified voting systems.

3. The Board cannot reasonably rely on Logic and Accuracy Testing for any level of assurance of machine accuracy in the wake of the numerous security failures in various areas of the system. As you know, the LAT procedure tests machine operations only in "test mode," and is not a reflection of whether the machine performs accurately in "election mode."

4. The barrage of recent national news with new information on the extent of Russian interference with 2016 elections cannot be ignored given the now proven open access to Georgia's system that existed in 2016 and until at least March 2017. The Board and Elections Director must fulfil their duty to conduct a secure election free from the threats of a compromised system.

5. Despite the Director's authority to order a paper ballot election given the known security threats to the DRE system and illegal system configuration, the Director abused her discretion by ignoring multiple expert warnings and conducting the election on a system she knew to be insecure and in violation of laws and regulations. Ms. Eveler was present for testimony in the June 7 Curling v. Kemp hearing, and received the pleadings in that case, and therefore had more than adequate knowledge of the dangers of the uncertified and compromised system to require that she employ paper ballots for the proper conduct of the election.

This list is not exhaustive, but provides overwhelming rationale that dictates that a certification of this election cannot be reasonably justified.

Thank you for your consideration in this matter. We are happy to provide further documentation of our concerns if it would be helpful to you in your deliberations.

Sincerely,

Marilyn Marks
Executive Director
Rocky Mountain Foundation

cc: Daniel W. White (dwhite@hlclaw.com )